UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JUSTIN SHERWOOD, individually and on behalf of all others similarly situated, **Plaintiff,** **v.** **HORIZON ACTUARIAL SERVICES, LLC,** **Defendant.**	**Case No.** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Justin Sherwood ("Plaintiff" or "Sherwood") brings this Class Action Complaint, on behalf of himself and all others similarly situated (the "Class") against Defendant Horizon Actuarial Services, LLC ("Defendant" or "Horizon") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF CASE

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession, custody and/or control of Defendant Horizon Actuarial Services, LLC (the "Data Breach").

2. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of Plaintiff's and Class Members' highly personal information called personal identifying information ("PII"), including names, Social Security Numbers, and dates of births.

3. The Data Breach occurred on or about November 10th and 11th of 2021. Despite occurring in November 2021, Horizon waited to begin informing Class Members until roughly January 13, 2022. Plaintiff did not receive his Notice of Data Incident from Horizon until April 14, 2022 (it was dated April 8, 2022) – more than 5 months after the Data Breach occurred. During this time, Plaintiff and Class Members were unaware that their sensitive personal identifying information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

4. Horizon failed to reasonably secure, monitor, and maintain the PII provided to it by its customers and business associates. Upon information and belief, the Data Breach resulted in the likely unauthorized access, download, exfiltration, and misuse of the PII by the cyber criminals who targeted that information through their wrongdoing.

5. The full extent of the types of PII, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant and its

agents, counsel, and forensic security vendors at this phase of the litigation.

6. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals, and knew or should have known that it was responsible for safeguarding and protecting Plaintiff's and Class Members' PII from unauthorized access, disclosure, and theft due to criminal hacking activity.

7. Upon information and belief, Defendant is responsible for allowing this Data Breach because of multiple acts of negligence, including but not limited to its: failure to design, implement, and maintain reasonable and adequate data security systems and safeguards, including but not limited to a lack of encryption; and/or its failure to exercise reasonable care in the hiring, supervision, and training of its employees, agents, and vendors; and/or its failure to comply with industry-standard data security practices; and/or its failure to comply with state and federal laws and regulations that govern data security and practices which are intended to protect the type of PII at issue in this action.

8. In this era of frequent data security attacks and data breaches, particularly in the financial industry, Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

9. Criminal hackers obtained Plaintiff's and Class Members' PII because

of its value in exploiting and stealing the identities of Plaintiff and the Class Members.

10. As a direct and proximate result of the Data Breach, Plaintiff and Class Members are now at a significant present and future risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come.

11. As a direct and proximate result of Defendant's data security failures and the Data Breach, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (v) the invasion of privacy; (vi) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and the Class Members' PII; and, (vii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII.

12. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

13. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

14. Accordingly, Plaintiff, on behalf of himself and other Class Members, asserts claims for Negligence (Count I), and Declaratory Judgment and Injunctive Relief (Count II).

PARTIES

Plaintiff Justin Sherwood

15. Plaintiff Justin Sherwood is, and at all times relevant has been, a resident and citizen of Nevada, and intends to remain a citizen of Nevada. Plaintiff received a "Notice of Data Breach" letter dated April 8, 2022 on April 14, 2022. The letter notified Plaintiff that on November 10 and 11, 2021, two of Horizon's computer servers were accessed by unauthorized actors and the certain PII was included in the files that were accessed including Plaintiff's name, date of birth and Social Security number.

Defendant Horizon Actuarial Services, LLC

16. Defendant Horizon Actuarial Services, LLC is organized under the laws of Delaware and has a principal place of business in Atlanta, Georgia. The members of Horizon as an LLC are the following individuals: (1) Stan Goldfarb, a citizen of Maryland; (2) Mary Ann Dunleavy, a citizen of Maryland; (3) Cary Franklin, a citizen of California; (4) Kathleen Coda, a citizen of California; (5) Ron Littler, a citizen of California; (6) Mark Lewis, a citizen of Georgia; (7) Nathan Slaff, a citizen of Georgia; and (8) Tom Cliffel, a citizen of Ohio.[1]

JURISDICTION AND VENUE

17. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the putative Class, as defined below, are citizens of a different state than Defendant Horizon, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs. For example, Plaintiff is a citizen of Nevada and none of the members of Horizon's LLC are citizens of Nevada.

[1] *See also* https://www.horizonactuarial.com/about-us.html (noting that Horizon "is an independent company operating as a limited liability corporation incorporated in the state of Delaware. It is owned and operated by its principals.") (Last visited on Apr. 17, 2022).

18. This Court has general personal jurisdiction over Horizon because its principal place of business at 1040 Crown Pointe Parkway, Suite 560, Atlanta, Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Defendant intentionally availed itself of this jurisdiction by marketing and selling products and services from Georgia to many businesses nationwide.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Horizon's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

Horizon Actuarial Services, LLC

20. Horizon began offering its actuarial services for multiemployer and Taft-Hartley plans on February 1, 2008. It boasts that is provides "superior actuarial and consulting services to multiemployer benefit plans – first as the Wyatt Company, then as Watson Wyatt, and now as Horizon Actuarial Services, LLC."[2] Furthermore, Horizon provides "a wide array of services related to defined benefit pension plans, including annual actuarial valuations, PPA compliance, plan design,

[2] *Id.*

asset-liability modeling, actuarial reviews, and merger and spin-off studies."[3]

21. As detailed more fully below, Horizon failed to safely and securely store the PII entrusted to it and failed to prevent it from being compromised during the Data Breach.

22. Horizon's website includes a link titled Notice of Data Incident.[4] The link states that Horizon "is providing notice of a data privacy incident on behalf of itself and the benefit plans listed below to whom Horizon Actuarial provides technical and actuarial consulting services (the 'Plans'). Horizon Actuarial received information regarding plan participants and their family members for business and compliance purposes." Those benefit plans include:

- Airconditioning and Refrigeration Industry & Welfare Trust Fund
- Airconditioning and Refrigeration Industry Retirement Trust Fund
- Fox Valley & Vicinity Labor Pension Plan
- Fox Valley & Vicinity Labor Welfare Plan
- Major League Baseball Players Benefit Plan
- National Hockey League Players Association Health and Benefits Fund
- National Roofing Industry Pension Plan, OCU Health & Welfare Trust
- OCU Pension Trust
- Operating Engineers Local 324 Pension Plan
- Patriot Retirees Voluntary Employees' Beneficiary Association
- Rocky Mountain UFCW Health Benefit Plan for Retired Employees

[3] *Id.*

[4] https://www.horizonactuarial.com/notice-of-data-incident.html (last visited on Apr. 17, 2022).

- Rocky Mountain UFCW Retail and Meat Pension Plan
- Roofers Local 20 Pension Plan
- Roofers Local No. 20 Health & Welfare Plan
- Teamsters Local 1034 Pension Fund
- Teamsters Local 27 Pension Fund
- Teamsters Local 295 Employers Group Welfare Trust
- Teamsters Local 813 Pension Fund
- Twin Cities Bakery Drivers Health & Welfare Fund
- Twin Cities Bakery Drivers Pension Fund
- UA Local 198 Pension Fund, UFCW & Employers Benefit Trust
- UFCW Comprehensive Benefit Trust
- UFCW Intermountain Health Fund
- UFCW Local 711 & Retail Food Employers Benefit Fund
- United Union of Roofers Burial Benefit Fund.[5]

23. Horizon's website confirmed PII was included in the Data Breach: "The investigation revealed that two Horizon Actuarial computer servers were accessed without authorization for a limited period on November 10 and 11, 2021. The group provided a list of information they claimed to have stolen. The types of information impacted may include names, dates of birth, Social Security numbers, and health plan information."[6]

[5] *Id.*
[6] *Id.*

24. Acknowledging deficiencies in its cybersecurity policies and procedures, Horizon had to implement additional security "measures to protect against similar incidents moving forward."[7]

25. Horizon, given the highly sensitive nature of the PII it possessed and the sensitivity of the actuarial services it provides, had a duty to safeguard, protect, and encrypt Plaintiff's and Class Members' PII.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

26. The PII of consumers, such as Plaintiff and Class Members, is valuable and has been commoditized in recent years.

27. Defendant was at all times fully aware of its obligations to protect Plaintiff's and Class Members' PII because of its business model of collecting PII and storing such information for the purpose of administering actuarial services for pecuniary gain. Defendant was also aware of the significant repercussions that would result from its failure to do so.

28. Horizon knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security were breached. Horizon failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

[7] *Id*.

29. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers when multiple types of information for a single user are combined. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identity theft and/or financial fraud.

30. According to the United States Cybersecurity & Infrastructure Security Agency:

> Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.[8]

31. Since these warnings, PII-related breaches have continued to rapidly increase, and yet, Defendant failed to exercise the reasonable care in hiring, training, and supervising its employees and agents to implement necessary data security and protective measures.

32. As such, Defendant should have not only known about the potential for

[8] https://www.cisa.gov/ransomware (last visited Apr. 16, 2021).

the data breach but should have taken steps to increase the security. Instead, Horizon relied on its outdated data security safeguards leading to the Data Breach.

33. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as a person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

34. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

35. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

36. According to the FBI's Internet Crime Complaint Center (IC3) 2020 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $4.1 billion in losses

to individuals and business victims.[9]

37. In 2020, as the COVID-19 global pandemic permeated all aspects of life, cyber fraudsters took the opportunity to exploit the pandemic and targeted both businesses and individuals.[10]

38. Data breaches facilitate identity theft as hackers obtain consumers' PII, thereafter using it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

39. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

40. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, many victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

---

[9] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Jan. 22, 2022).
[10] *Id.*

41. Further complicating the issues faced by victims of identity theft, data thieves often wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and Class Members (and the business entities whose information was breached) will need to be remain vigilant against unauthorized data use for years or even decades to come.

42. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point: Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.

43. Recognizing the high value consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives the information. And, by making the transaction transparent, consumers—not criminals—will be compensated.[11]

[11] *See* Steve Lohr, You Want My Personal Data? Reward Me for It, The New York Times, *available at* http://www.nytimes.com/2010/07/18/business/18unboxed.html (last accessed Jan 22, 2022).

44. Consumers place a high value on their PII, in addition to the privacy of same. Research shows how much consumers value their data privacy, and the amount is considerable.

45. By virtue of the Data Breach here and unauthorized release and disclosure of the PII of Plaintiff and the Class, Defendant has deprived Plaintiff and Class Members of the substantial value of their PII, to which they are entitled. As previously alleged, Defendant failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

46. According to the FTC, unauthorized PII disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[12]

47. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

48. Even absent any adverse use, consumers suffer injury from the simple

[12] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last accessed Jan. 22, 2021).

fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

49. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiff's and other Class Members' PII, Plaintiff and all Class Members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; (iii) out-of-pocket expenses for securing identity theft protection and other similar necessary services; and (iv) emotional distress as a result of having their PII impacted in the Data Breach.

FTC Guidelines Prohibit Unfair or Deceptive Acts

50. Horizon is prohibited by the Federal Trade Commission Act, 15 U.S.C.

§ 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

51. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[13]

52. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[14]

53. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for

[13] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 22, 2022).
[14] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136proteting-personal-information.pdf (last visited Jan. 22, 2022).

security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[15]

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. Horizon failed to properly implement basic data security practices. Horizon's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

56. Horizon was at all times fully aware of its obligations to protect Plaintiff's and Class Members' PII because of its business model of collecting PII and storing such information for analysis and for pecuniary gain. Horizon was also aware of the significant repercussions that would result from its failure to do so.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

57. At all relevant times, Defendant knew, or reasonably should have

[15] *Id.*

known, of the importance of safeguarding PII and of the foreseeable consequences if its data security, or agent's data security systems were breached, including the significant costs that would be imposed on Plaintiff and the Class as a result of the breach.

58. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

59. As a result of the Breach, Plaintiff and the other Class Members must now be vigilant and review their credit reports for suspected incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft. The need for additional monitoring for identity theft and fraud will extend indefinitely into the future.

60. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

61. Plaintiff and the other Class Members have suffered and will suffer actual injury due to loss of time and increased risk of identity theft as a direct result of the Breach. In addition to fraudulent charges, loss of use of and access to their account funds, costs associated with their inability to obtain money from their accounts, diminution of value of the data, and damage to their credit, Plaintiff and the other Class Members suffer ascertainable losses in the form of out-of-pocket expenses, opportunity costs, and the time and costs reasonably incurred to remedy or mitigate the effects of the Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the financial information in possession of Defendant;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

L. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

62. Moreover, Plaintiff and the other Class Members have an interest in ensuring that Defendant implement reasonable security measures and safeguards to maintain the integrity and confidentiality of the PII, including making sure that the storage of data or documents containing PII is not accessible by unauthorized persons and that access to such data is sufficiently protected.

63. And finally, as a direct and proximate result of Defendant's actions and inactions, Plaintiff and the other Class Members have suffered out-of-pocket losses, anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

64. In addition to the remedy for economic harm, Plaintiff and the Class Members maintain an undeniable and continuing interest in ensuring that the PII remains in the possession of Defendant is secure, remains secure, and is not subject

to future theft.

Plaintiff Justin Sherwood's Experience

65. Plaintiff typically takes measures to protect his PII and is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

66. Plaintiff stores any documents containing his PII in a safe and secure location. Sherwood also diligently chooses unique usernames and passwords for his online accounts.

67. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress as a result of worrying about his PII being exfiltrated. He has monitored his Credit Karma account extensively since receiving the Notice of Data Incident from Defendant, and intends to spend time taking steps to protect his PII. This is time that was and will be lost and unproductive and taken away from other activities and duties.

68. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety, emotional distress, and increased concerns for the loss of his privacy.

69. As a result of the Data Breach and the exfiltration of his unencrypted PII in the hands of criminals, Plaintiff is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

70. To date, Defendant has done very little to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach. It offered identity monitoring services, but only for one year, which is wholly inadequate for a data breach including Plaintiff's and Class Members' Social Security numbers.

CLASS DEFINITION AND ALLEGATIONS

71. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following classes:

The Class:

> **All persons residing in the United States who had their PII hosted by Horizon compromised as a result of the Data Breach.**

72. Excluded from the Class are: (i) Defendant and its officers, directors, affiliates, parents, and subsidiaries; (ii) the Judge presiding over this action; and (iii) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding, or abetting the criminal activity occurrence of

the Data Breaches.

73. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

74. **Numerosity**. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believe that the proposed Class includes over 100,000 individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

75. **Commonality and Predominance**. This action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. These common legal and factual questions include, but are not limited to, the following:

a. whether Defendant engaged in the wrongful conduct alleged herein;

b. whether the alleged conduct constitutes violations of the laws asserted;

c. whether Defendant owed Plaintiff and the other Class Members a duty to adequately protect their PII;

d. whether Defendant breached its duty to protect the PII of Plaintiff and the other Class Members;

e. whether Defendant knew or should have known about the inadequacies of its data protection, storage, and security;

f. whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and the other Class Members' PII from unauthorized theft, release, or disclosure;

g. whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems and digital storage environment;

h. whether Defendant had the proper computer systems to safeguard and protect Plaintiff's and the other Class Members' PII from unauthorized theft, release or disclosure;

i. whether Defendant breached the promise to keep Plaintiff's and the Class Members' PII safe and to follow federal data security protocols;

j. whether Defendant's conduct was the proximate cause of Plaintiff's and the other Class Members' injuries;

k. whether Defendant took reasonable measures to determine the

extent of the Data Breach after it was discovered;

l. whether Plaintiff and the other Class Members suffered ascertainable and cognizable injuries as a result of Defendant's conduct;

m. whether Plaintiff and the other Class Members are entitled to recover actual damages and/or statutory damages; and,

n. whether Plaintiff and the other Class Members are entitled to other appropriate remedies, including injunctive relief.

76. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of themselves and the other Class Members. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

77. **Typicality**. Plaintiff's claims are typical of the claims of the members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class Members in a similar manner.

78. **Adequacy**. Plaintiff will fairly and adequately protect the interests of the Members of the Class, have retained counsel experienced in complex consumer class action litigation, and intend to prosecute this action vigorously. Plaintiff has

no adverse or antagonistic interests to those of the Class.

79. **Superiority**. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class Members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision a single court, and presents no unusual management difficulties under the circumstances here.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

80. Plaintiff restates and realleges all proceeding factual allegations above and hereafter as if fully set forth herein.

81. Upon gaining access to the PII of Plaintiff and Members of the Class, Defendant owed to Plaintiff and the Class a common law duty of reasonable care in

handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties. Pursuant to this duty, Defendant was required to design, maintain, and test its security systems to ensure that these systems were reasonably secure and capable of protecting the PII of Plaintiff and the Class. Defendant further owed to Plaintiff and the Class a duty to implement systems and procedures that would detect a breach of its security systems in a timely manner and to timely act upon security alerts from such systems.

82. Defendant owed this duty to Plaintiff and the other Class Members because Plaintiff and the other Class Members compose a well-defined, foreseeable, and probable class of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols. Defendant actively solicited clients who entrusted Defendant with Plaintiff's and the other Class Members' PII when obtaining and using Defendant's services. To facilitate these services, Defendant used, handled, gathered, and stored the PII of Plaintiff and the other Class Members. Attendant to Defendant's solicitation, use and storage, Defendant knew of its inadequate and unreasonable security practices with regard to its computer/server systems and also knew that hackers and thieves routinely attempt to access, steal and misuse the PII that Defendant actively solicited from clients who entrusted Defendant with Plaintiff's and the other Class Members' data.

As such, Defendant knew a breach of its systems would cause damage to its clients and Plaintiff and the other Class Members.

83. Defendant breached its duty to Plaintiff and the other Class Members by failing to implement and maintain security controls that were capable of adequately protecting the PII of Plaintiff and the other Class Members.

84. Defendant also breached its duty to timely and accurately disclose to Plaintiff and the other Class Members that their PII had been or was reasonably believed to have been improperly accessed or stolen.

85. Defendant's negligence in failing to exercise reasonable care in protecting the PII of Plaintiff and the other Class Members is further evidenced by Defendant's failure to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when the Data Breach was disclosed.

86. Furthermore, Defendant was negligent for waiting for more than five months to notify Plaintiff and similarly situated Class Members of the Data Breach.

87. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA") Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Defendant to take reasonable measures to protect Plaintiff's and the Class Member's PII data and is a further source of Defendant's duty to Plaintiff and

the Class Members. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to implement and use reasonable measures to protect Sensitive Information. Defendant, therefore, was required and obligated to take reasonable measures to protect PII it solicited, possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendant's duty to adequately protect Sensitive Information. By failing to implement and use reasonable data security measures, Defendant acted in violation of § 5 of the FTCA.

88. Defendant is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Defendant to exercise reasonable care with respect to Plaintiff and the Class Members by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class Members. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, Defendant was the only entity capable of adequately protecting the data that that it alone solicited, collected, and stored.

89. The injuries to Plaintiff and the other Class Members were reasonably foreseeable to Defendant because common law, statutes, and industry standards

require Defendant to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiff's and the other Class Members' PII.

90. The injuries to Plaintiff and the other Class Members also were reasonably foreseeable because Defendant knew or should have known that systems used for safeguarding PII were inadequately secured and exposed consumer PII to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, Defendant's own misconduct created a foreseeable risk of harm to Plaintiff and the other Class Members.

91. Defendant's failure to take reasonable steps to protect the PII of Plaintiff and the other members of the Class was a proximate cause of their injuries because it directly allowed thieves easy access to Plaintiff's and the other Class Members' PII. This ease of access allowed thieves to steal PII of Plaintiff and the other Class Members, which could lead to dissemination in black markets.

92. As a direct proximate result of Defendant's conduct, Plaintiff and the other Class Members have suffered theft of their PII. Defendant allowed thieves access to Plaintiff's and Class Members' PII, thereby decreasing the security of Plaintiff's and Class Members' financial and personal accounts, making Plaintiff's and Class Members' identities less secure and reliable, and subjecting Plaintiff's

and Class Members to the imminent threat of identity theft. Not only will Plaintiff and the other members of the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

93. Defendant's conduct warrants moral blame because Defendant actively solicited its services to its clients, wherein it used, handled, and stored the PII of Plaintiff and the other Class Members without disclosing that its security was inadequate and unable to protect the PII of Plaintiff and the other Class Members. Holding Defendant accountable for its negligence will further the policies embodied in such law by incentivizing IT service providers to properly secure sensitive consumer information and protect the consumers who rely on these companies every day.

94. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as described herein and throughout this Complaint, and are entitled to damages, including compensatory, and punitive damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

95. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

96. Defendant's unreasonable data security measures and failure to timely notify Plaintiff and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which Defendant failed to do.

97. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to implement and use reasonable measures to protect users' sensitive data. The FTC publications and orders described above also form the basis of Defendant's duty.

98. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the sensitive nature and amount of data it stored and the foreseeable consequences of a Data Breach should Defendant fail to secure its systems.

99. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

100. Plaintiffs and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiffs and the Class.

101. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and the Class have suffered and continue to suffer injury.

THIRD CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class)

102. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

103. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

104. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' Sensitive Information, including whether Horizon is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Sensitive Information. Plaintiff alleges that Horizon's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

105. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Horizon owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act; and

b. Horizon breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Sensitive Information.

c. Horizon's breach of its legal duty continues to cause harm to Plaintiff and the Class Members.

106. This Court also should issue corresponding injunctive relief requiring Horizon to employ adequate security protocols consistent with law and industry standards to protect consumers' (Plaintiff's and the Class Members') Sensitive Information.

107. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Horizon. The risk of another such breach is real, immediate, and substantial. If another breach at Horizon occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits to rectify the same conduct. Monetary damages, while warranted to compensate Plaintiff and

the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class Members.

108. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Horizon if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Horizon of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Horizon has pre-existing legal obligations to employ such measures.

109. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Horizon, thus eliminating the additional injuries that would result to Plaintiff, Class Members and consumers whose PII would be further compromised.

FOURTH CAUSE OF ACTION
VIOLATION OF O.C.G.A. § 13-6-11
(On behalf of the Nationwide Class)

110. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

111. Defendant through its actions alleged and described herein acted in bad faith, were stubbornly litigious, or caused Plaintiff and Class Members unnecessary trouble and expense with respect to the events underlying this litigation.

112. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to implement and use reasonable measures to protect Sensitive Information. Various FTC publications and orders also form the basis of Defendant's duty.

113. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII that it obtained and stored and the foreseeable consequences of a data breach.

114. Defendant also has a duty under the Georgia Constitution ('the Constitution') which contains a Right to Privacy clause, Chapter 1, Article 1, to protect its users' private information. The Georgia Constitution states "no person shall be deprived of life, liberty, or property except by due process of law." Moreover, the Georgia Constitution identifies certain invasions of privacy, including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

115. This duty has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) §652A which specifically recognized four common law invasion of privacy claims in Georgia, which include 1) appropriation of likeness; 2) intrusion on solitude or seclusion; 3) public disclosure of private facts; and 4) false light.

116. Defendant's implementation of inadequate data security measures, its failure to resolve vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect data it required Plaintiff and Class Members to provide and stored on its own servers and databases constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

117. Defendant knew or should have known that it had a responsibility to protect the PII it possessed for Plaintiff and Class Members and stored, that it was entrusted with this Sensitive Information, and that it was the only entities capable of adequately protecting the PII.

118. Despite that knowledge, Defendant abdicated its duty to protect the PII it required Plaintiff and Class Members provide and that it stored.

119. As a direct and proximate result of Defendant's actions, Plaintiff's and the Class Members' PII was stolen. As further alleged above, the Data Breach was a direct consequence of Horizon's abrogation of data security responsibility and its

decision to employ knowingly deficient data security measures that knowingly left the PII unsecured. Had Horizon adopted reasonable data security measures, it could have prevented the Data Breach.

120. As further described above, Plaintiff and the Class Members have been injured and suffered losses directly attributable to the Data Breach.

121. Plaintiff and Class Members therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representatives of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses pursuant to O.C.G.A. § 13-6-11 and as otherwise allowed by law;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff Justin Sherwood individually and on behalf of the the putative Class, demand a trial by jury on all claims so triable.

Respectfully Submitted,

THE FINLEY FIRM, P.C.
/s/ MaryBeth V. Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
N. Nickolas Jackson
Georgia Bar No. 841433
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Telephone: (404) 320-9979
Fax: (404) 320-9978

mgibson@thefinleyfirm.com
njackson@thefinleyfirm.com

Terence R. Coates*
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Plaintiff's and Putative Class Counsel

*** Pro Have Vice Forthcoming*